Building Automation Systems

An Overview Including Dragos Solutions

Daniel Gaeta
Zach Spencer

Zach Spencer

Senior Enterprise Account Manager

linkedin.com/in/Zachary-spencer

- 1 Year @ Dragos and 8 Years in industry
- Previous roles in Building Automation cybersecurity, sales, system integration, and engineering
- Experience securely integrating multi-national ICS/OT networks
- BS Chemical Engineering | Previous roles at Carrier, Honeywell, and Siemens

Daniel Gaeta

linkedin.com/in/dangaeta

Senior Solutions Architect

- 2 Years @ Dragos and 15 Years in industry, with roles in OT/ICS system cybersecurity, engineering, operations, and maintenance
- Past titles include Federal Industrial Control Systems Cybersecurity Technologist, Senior Principle Cyber Systems Engineer, Facilities O&M Mechanical Lead, and Infrastructure Mechanical Engineer
- BSME from UCCS | Previous roles with Northrop Grumman at the Missile Defense Agency and Jacobs

GICSP

CISSP

IFMA fmp Facility Management Professional

AGENDA OUTLINE

1. Industry Terminology
2. Business Impact of Cyber Threats in BAS
3. Threat Scenarios
4. Dragos Platform BAS Scenario Demos
5. Case Study Highlights
6. Dragos BAS Solutions and Resources

BUILDING TERMINOLOGY

BUILDING MANAGEMENT SYSTEMS (BMS)

BUILDING AUTOMATION SYSTEMS (BAS)

BUILDING CONTROL SYSTEM (BCS)

FACILITY RELATED CONTROL SYSTEMS (FRCS)

These refer to generally similar systems

For simplicity, we’ll use BAS as the standard term

BAS EXAMPLES

EMCS

ENERGY MANAGEMENT & CONTROL SYSTEM

Control and monitor anything related to energy (electric or otherwise)

HVAC

HEATING, VENTILATION, AIR CONDITIONING

Temp/humidity, fans, dampers, air handling units, purification

FLS

FIRE AND LIFE SAFETY

Fire detection and suppression, sprinklers, audible announcement

ESS

ELECTRONIC SECURITY SYSTEMS

Including physical security, access control, cameras, perimeter monitoring

MECH

MECHANICAL

Water pumps, hydraulic flow, temperature, boilers, black/grey water

ELEV

ELEVATORS

Destination dispatch, transport control, video display

POTENTIAL BUSINESS IMPACT

Building Automation Systems

Human Safety

Camera monitoring,
physical access,
mechanical failures

Brand Reputation

customer confidence,
stock value

Legal and Compliance

IP Protection, PII

Protect Revenue

Customer obligations: working doors, elevators, security, cooling/heating

Non-tenant: e.g. Empire State Building is significant source of tourism revenue

Prevent Larger Security Incident

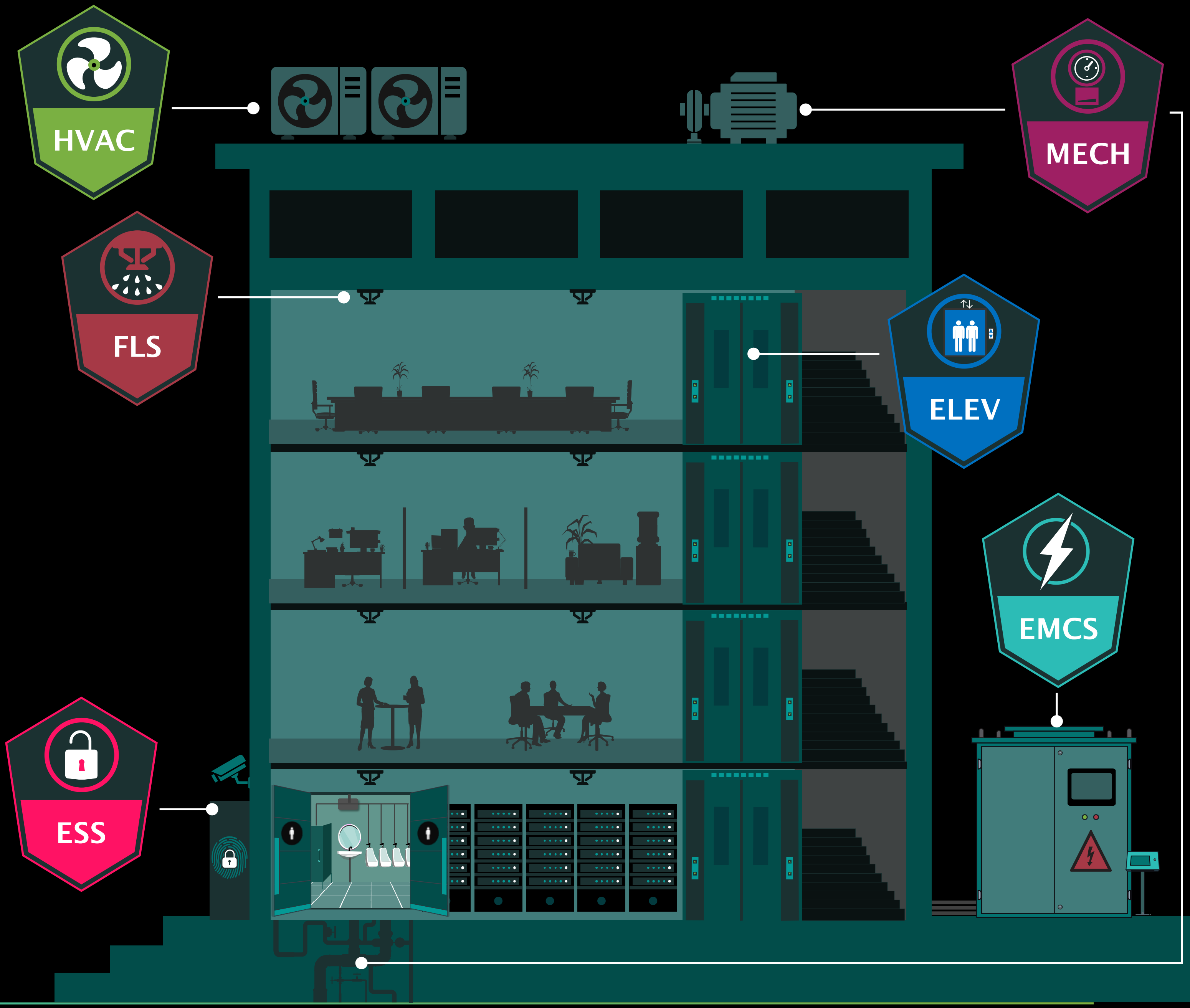
Pivot into IT enterprise,
or from IT into BAS or OT

BAS Threat Considerations:

1. BAS systems often connected to same network but protected by *different* teams and/or controls

2. One system compromised likely *exposes others*

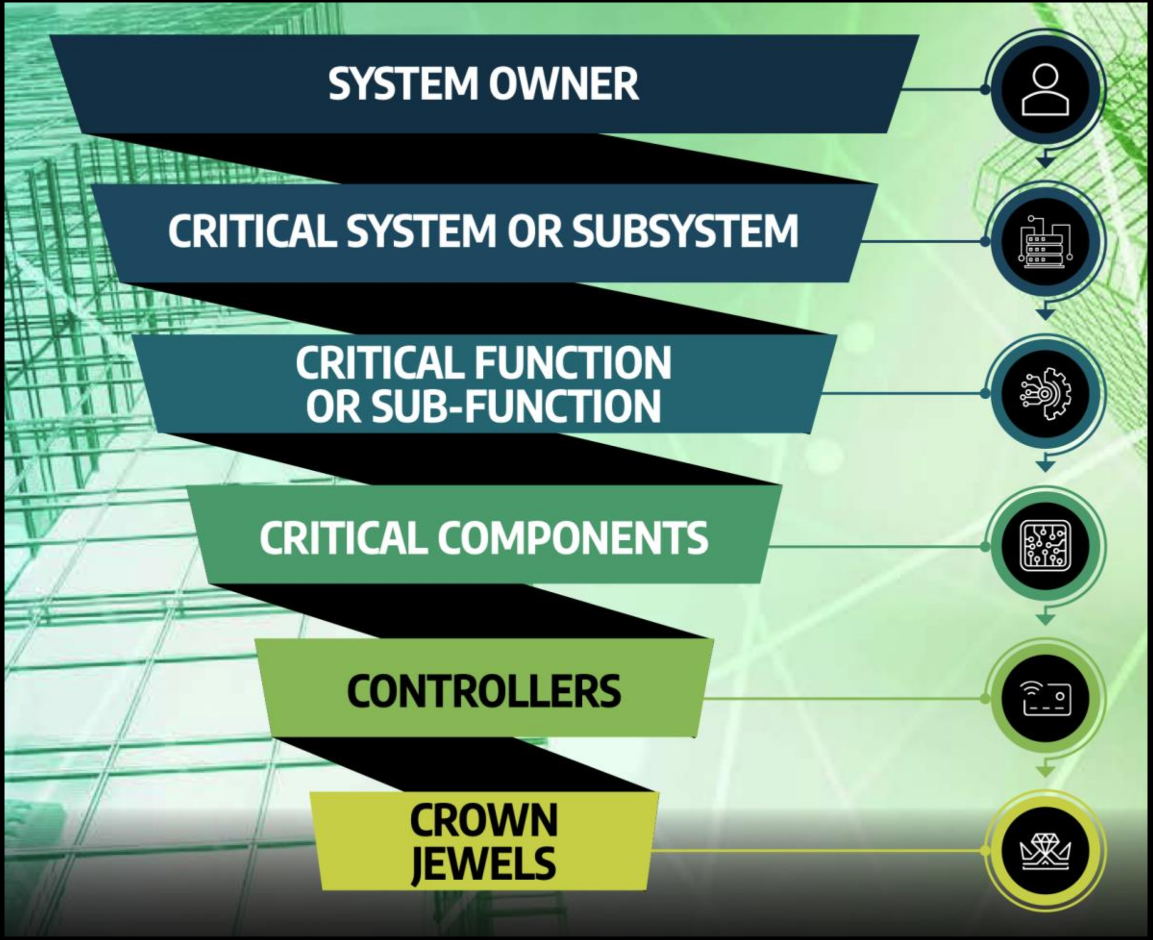
3. Loss of use for one system can have a *cascading effect*



DRAGOS

CROWN JEWEL ANALYSIS

- Crown Jewel Analysis (CJA) is an iterative process that works top-down to identify critical assets required for primary system function.
- Enables every aspect of vulnerability management, incident response, disaster recovery, and where detection and protection should be prioritized.

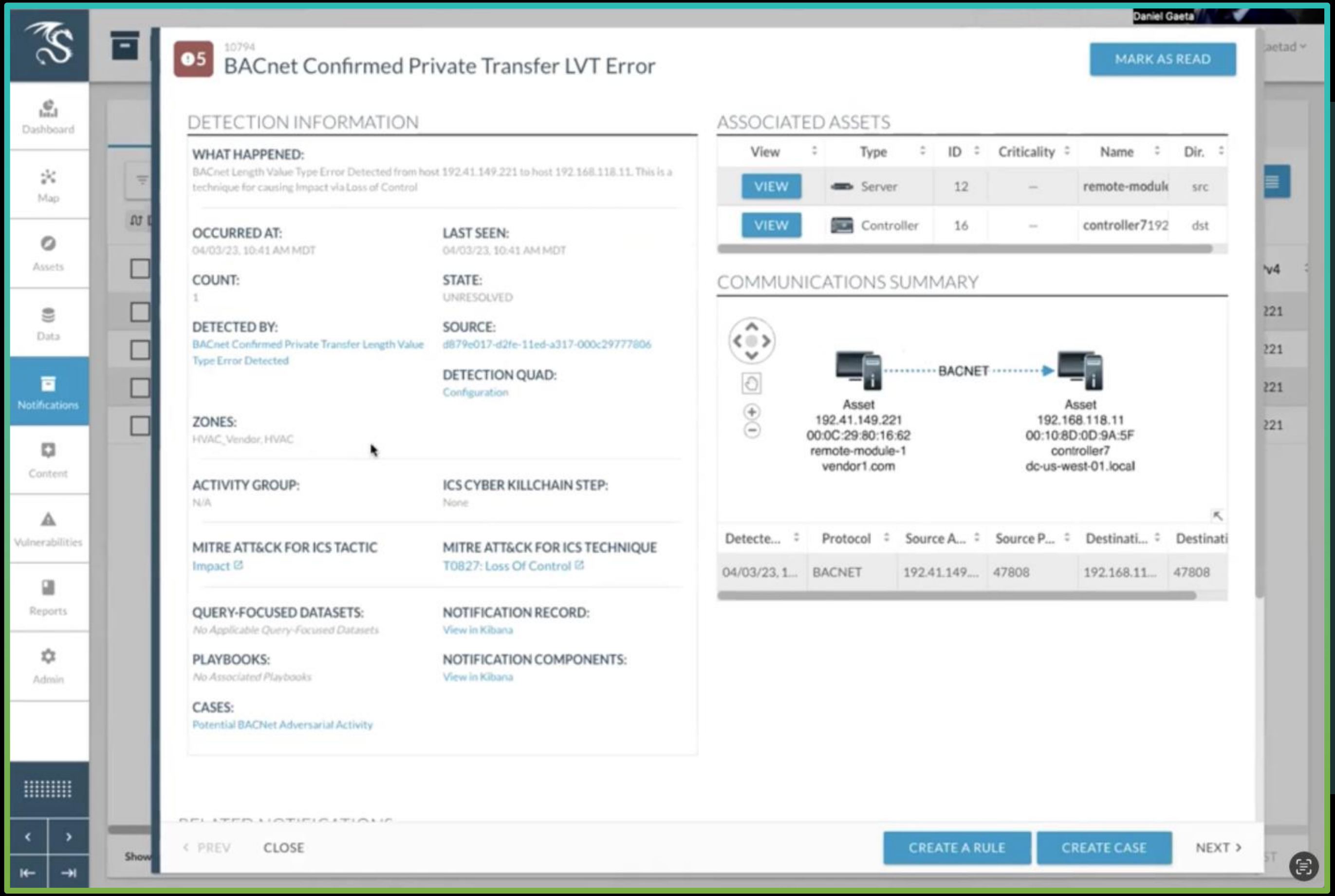

SYSTEM OWNER
CRITICAL SYSTEM OR SUBSYSTEM
CRITICAL FUNCTION OR SUB-FUNCTION
CRITICAL COMPONENTS
CONTROLLERS
CROWN JEWELS

DRAGOS PLATFORM – BAS THREAT SCENARIOS

1. BACnet Adversarial Activity
2. Authentication Brute Force Attempts
3. Ransomware IOC Detection

DRAGOS PLATFORM – BAS THREAT SCENARIOS

BACnet Adversarial Activity



10794

5 BACnet Confirmed Private Transfer LVT Error

DETECTION INFORMATION

WHAT HAPPENED:
BACnet Length Value Type Error Detected from host 192.41.149.221 to host 192.168.118.11. This is a technique for causing Impact via Loss of Control

OCCURRED AT: 04/03/23, 10:41 AM MDT

LAST SEEN: 04/03/23, 10:41 AM MDT

COUNT: 1

STATE: UNRESOLVED

DETECTED BY: BACnet Confirmed Private Transfer Length Value Type Error Detected

SOURCE: d879e017-d2fe-11ed-a317-000c29777806

DETECTION QUAD: Configuration

ZONES: HVAC_Vendor, HVAC

ACTIVITY GROUP: N/A

ICS CYBER KILLCHAIN STEP: None

MITRE ATT&CK FOR ICS TACTIC: Impact

MITRE ATT&CK FOR ICS TECHNIQUE: T0827: Loss Of Control

QUERY-FOCUSED DATASETS: *No Applicable Query-Focused Datasets*

NOTIFICATION RECORD: View in Kibana

PLAYBOOKS: *No Associated Playbooks*

NOTIFICATION COMPONENTS: View in Kibana

CASES: Potential BACNet Adversarial Activity

ASSOCIATED ASSETS

View	Type	ID	Criticality	Name	Dir.
VIEW	Server	12	–	remote-modul	src
VIEW	Controller	16	–	controller7192	dst

COMMUNICATIONS SUMMARY

Asset 192.41.149.221 00:0C:29:80:16:62 remote-module-1 vendor1.com ··· BACNET ···> Asset 192.168.118.11 00:10:8D:0D:9A:5F controller7 dc-us-west-01.local

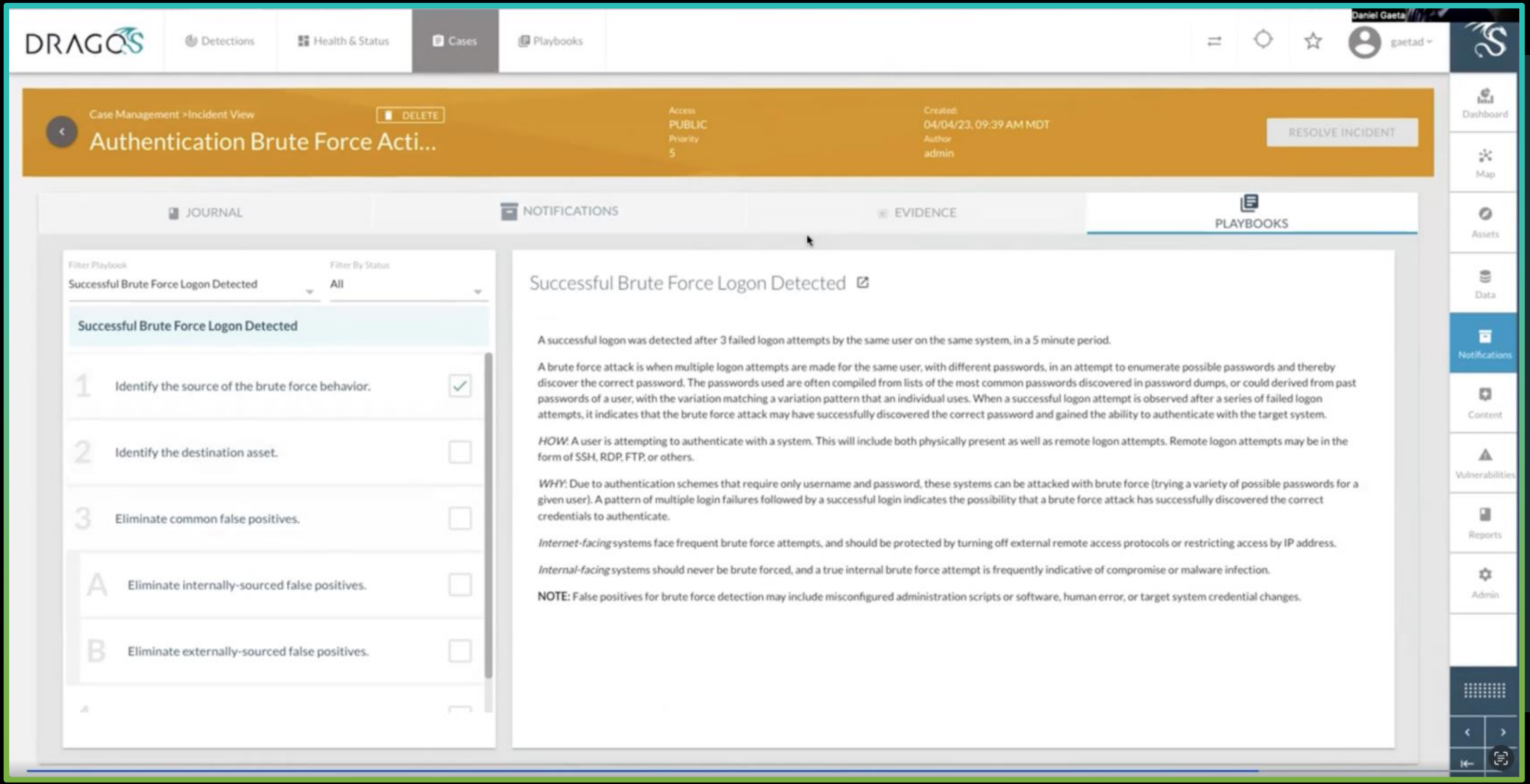
Detecte...	Protocol	Source A...	Source P...	Destinati...	Destinati
04/03/23, 1...	BACNET	192.41.149....	47808	192.168.11...	47808

- BACnet Confirmed Private Transfer LVT Error detection was triggered
- Upon further review, it is determined that the source asset involved is a vendor asset and abnormal (Nmap) activity was observed

Demo
Threat Scenario 1

DRAGOS PLATFORM – BAS THREAT SCENARIOS

Authentication Brute Force Attempts from Enterprise into IDMZ



Case Management >Incident View

Authentication Brute Force Acti...

Access: PUBLIC
Priority: 5

Created: 04/04/23, 09:39 AM MDT
Author: admin

Filter Playbook: Successful Brute Force Logon Detected
Filter By Status: All

Successful Brute Force Logon Detected

1 Identify the source of the brute force behavior. ☑

2 Identify the destination asset. □

3 Eliminate common false positives. □

A Eliminate internally-sourced false positives. □

B Eliminate externally-sourced false positives. □

Successful Brute Force Logon Detected

A successful logon was detected after 3 failed logon attempts by the same user on the same system, in a 5 minute period.

A brute force attack is when multiple logon attempts are made for the same user, with different passwords, in an attempt to enumerate possible passwords and thereby discover the correct password. The passwords used are often compiled from lists of the most common passwords discovered in password dumps, or could derived from past passwords of a user, with the variation matching a variation pattern that an individual uses. When a successful logon attempt is observed after a series of failed logon attempts, it indicates that the brute force attack may have successfully discovered the correct password and gained the ability to authenticate with the target system.

HOW: A user is attempting to authenticate with a system. This will include both physically present as well as remote logon attempts. Remote logon attempts may be in the form of SSH, RDP, FTP, or others.

WHY: Due to authentication schemes that require only username and password, these systems can be attacked with brute force (trying a variety of possible passwords for a given user). A pattern of multiple login failures followed by a successful login indicates the possibility that a brute force attack has successfully discovered the correct credentials to authenticate.

Internet-facing systems face frequent brute force attempts, and should be protected by turning off external remote access protocols or restricting access by IP address.

Internal-facing systems should never be brute forced, and a true internal brute force attempt is frequently indicative of compromise or malware infection.

NOTE: False positives for brute force detection may include misconfigured administration scripts or software, human error, or target system credential changes.

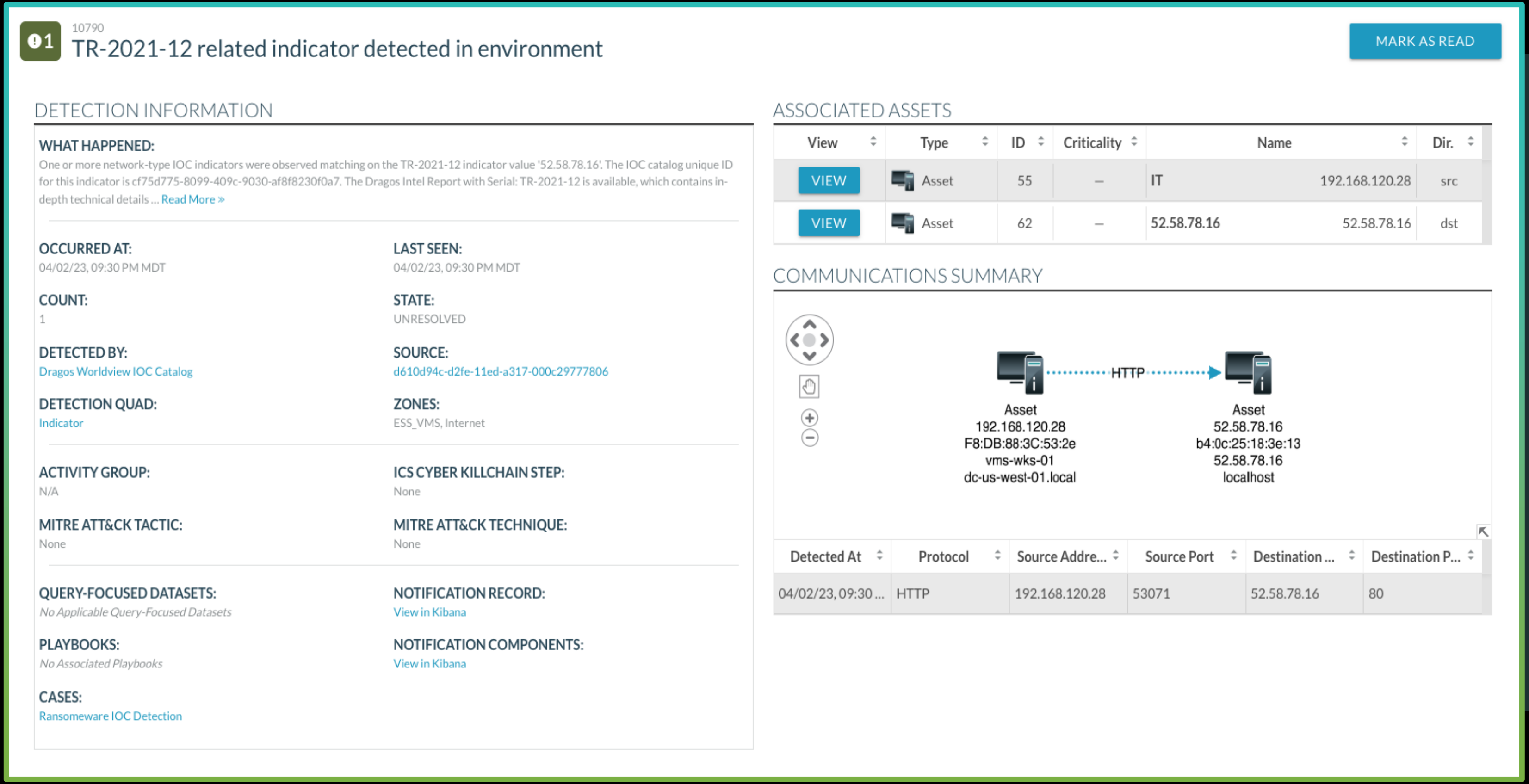
- Successful logon was detected after 3 failed logon attempts by the same user on the same system, in a 5-minute period.

- After additional investigation, it was determined that a mixture of default, domain, and local accounts were used in an attempt to gain access to the Historian.

Demo
Threat Scenario 2

DRAGOS PLATFORM – BAS THREAT SCENARIOS

Ransomware IOC Detection



10790

❶1 TR-2021-12 related indicator detected in environment

MARK AS READ

DETECTION INFORMATION

WHAT HAPPENED:
One or more network-type IOC indicators were observed matching on the TR-2021-12 indicator value '52.58.78.16'. The IOC catalog unique ID for this indicator is cf75d775-8099-409c-9030-af8f8230f0a7. The Dragos Intel Report with Serial: TR-2021-12 is available, which contains in-depth technical details ... Read More »

OCCURRED AT:
04/02/23, 09:30 PM MDT

LAST SEEN:
04/02/23, 09:30 PM MDT

COUNT:
1

STATE:
UNRESOLVED

DETECTED BY:
Dragos Worldview IOC Catalog

SOURCE:
d610d94c-d2fe-11ed-a317-000c29777806

DETECTION QUAD:
Indicator

ZONES:
ESS_VMS, Internet

ACTIVITY GROUP:
N/A

ICS CYBER KILLCHAIN STEP:
None

MITRE ATT&CK TACTIC:
None

MITRE ATT&CK TECHNIQUE:
None

QUERY-FOCUSED DATASETS:
No Applicable Query-Focused Datasets

NOTIFICATION RECORD:
View in Kibana

PLAYBOOKS:
No Associated Playbooks

NOTIFICATION COMPONENTS:
View in Kibana

CASES:
Ransomeware IOC Detection

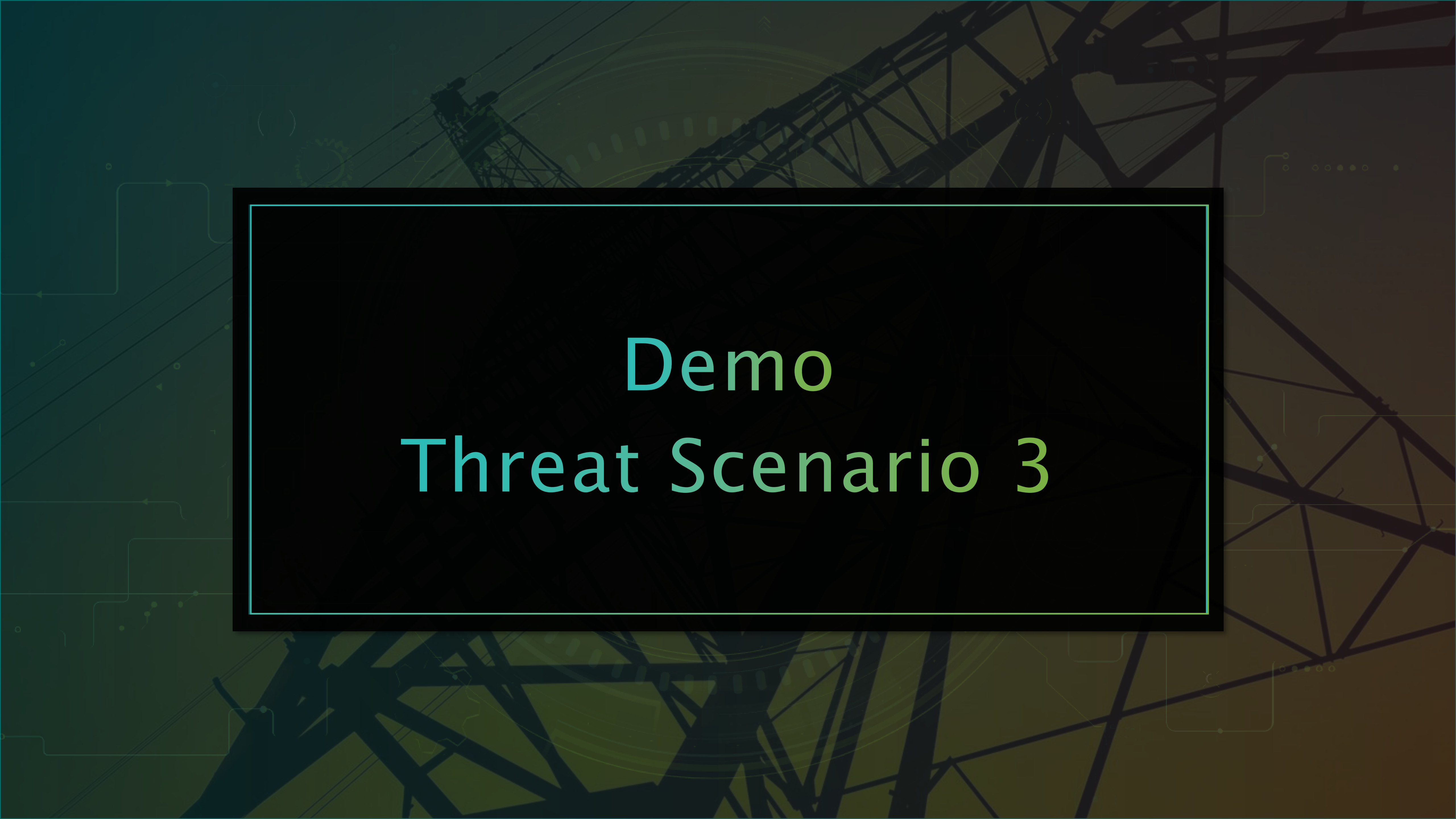
ASSOCIATED ASSETS

View	Type	ID	Criticality	Name	Dir.
VIEW	Asset	55	–	IT 192.168.120.28	src
VIEW	Asset	62	–	**52.58.78.16** 52.58.78.16	dst

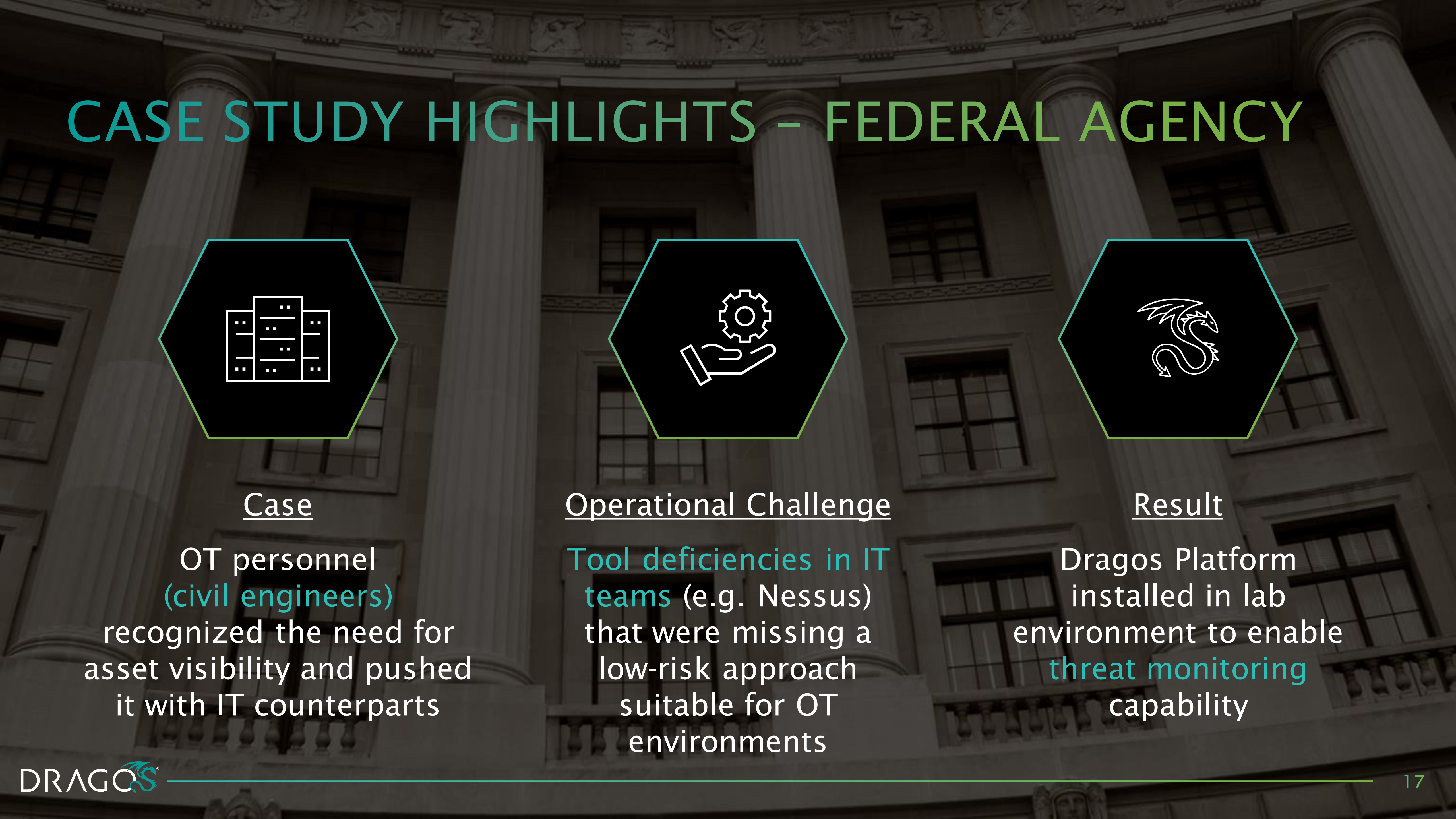
COMMUNICATIONS SUMMARY

Detected At	Protocol	Source Addre...	Source Port	Destination ...	Destination P...
04/02/23, 09:30 ...	HTTP	192.168.120.28	53071	52.58.78.16	80

- Ransomware IOC Detection (TR-2021-12) fires in the ESS_VMS zone.
- The company IRP is activated and Dragos IRR is engaged to respond



Demo
Threat Scenario 3



CASE STUDY HIGHLIGHTS – FEDERAL AGENCY

Case

OT personnel (civil engineers) recognized the need for asset visibility and pushed it with IT counterparts

Operational Challenge

Tool deficiencies in IT teams (e.g. Nessus) that were missing a low-risk approach suitable for OT environments

Result

Dragos Platform installed in lab environment to enable threat monitoring capability

CASE STUDY HIGHLIGHTS – TIER 1 TECH COMPANY

Case

Dragos professional services brought in for assessments and penetration tests

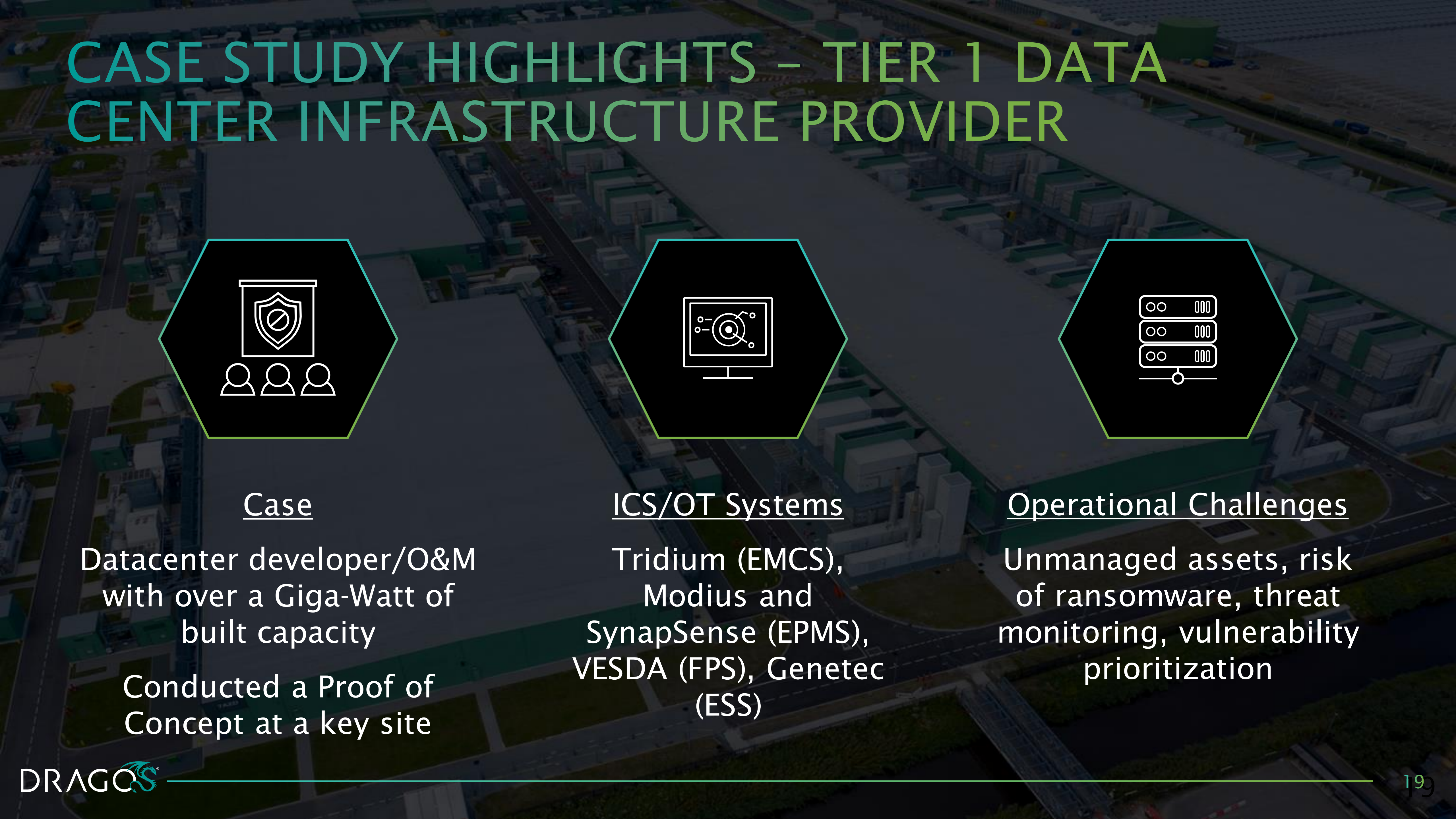
Looked at EPMS meters, Data Center Infra Mgmt Systems

ICS/OT Systems

Schneider and Eaton sensors/controllers (EMCS/EPMS), HVAC and mechanical systems

Operational Challenges

Dual homed servers, network segmentation issues, publicly exposed BAS systems, protocol manipulation over BACnet/Modbus



CASE STUDY HIGHLIGHTS – TIER 1 DATA CENTER INFRASTRUCTURE PROVIDER

Case

Datacenter developer/O&M with over a Giga-Watt of built capacity

Conducted a Proof of Concept at a key site

ICS/OT Systems

Tridium (EMCS), Modius and SynapSense (EPMS), VESDA (FPS), Genetec (ESS)

Operational Challenges

Unmanaged assets, risk of ransomware, threat monitoring, vulnerability prioritization

Effective OT Security

SANS

5 THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Monitoring Visibility

04
Secure Remote Access

05
Risk-based Vulnerability Management

DRAGOS SOLUTIONS

Dragos Platform

- Asset inventory
- Network monitoring
- Threat detection
- Vulnerability management

Global Services

- Architecture Review
- Network Vulnerability Assessment
- Readiness Assessment
- Penetration Testing
- Threat Hunting (OT Watch)
- Incident Response (RRR)
- Tabletop Exercise

Worldview Threat Intelligence

- Critical alerts
- Industry threat perspectives
- Weekly reports
- Executive insights
- Threat feed

DRAGOS RESOURCES ON BAS

INFOGRAPHIC

DRAGOS

INFOGRAPHIC

Securing Your Most Critical Building Automation Systems

Identifying and protecting the crown jewels in your facilities

DOWNLOAD NOW

CROWN JEWEL ANALYSIS

SYSTEM OWNER
CRITICAL SYSTEM OR SUBSYSTEM
CRITICAL FUNCTION OR SUB-FUNCTION
CRITICAL COMPONENTS
CONTROLLERS
CROWN JEWELS

SECTOR: BUILDING AUTOMATION SYSTEMS

Crown Jewel Analysis (CJA) is an iterative process that works top-down to systematically determine the physical & logical assets, data, and communication and control interfaces required for primary system function. Knowing the specific devices required for operations enables every aspect of vulnerability management, incident response, disaster recovery, and where detection and protection should be prioritized.

Building Automation Systems (BAS) are commonly found in Data Centers to handle the work of managing and recording data for managing various building systems. Additionally, BAS administrators can adjust the operation of these systems automatically to maximize the uptime and the operating efficiency. There are a few areas where BAS can play an important role in the data center.

Below is a simplified example of a Crown Jewel Analysis for typical building systems found within a co-location data center. Categori

and some products could be placed

WHITEPAPER

WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Assessing Operational Technology (OT) Cybersecurity Maturity

An Analysis of Leased Datacenters Utilizing the Cybersecurity Maturity Model Certification (CMMC)

SOLUTION BRIEF

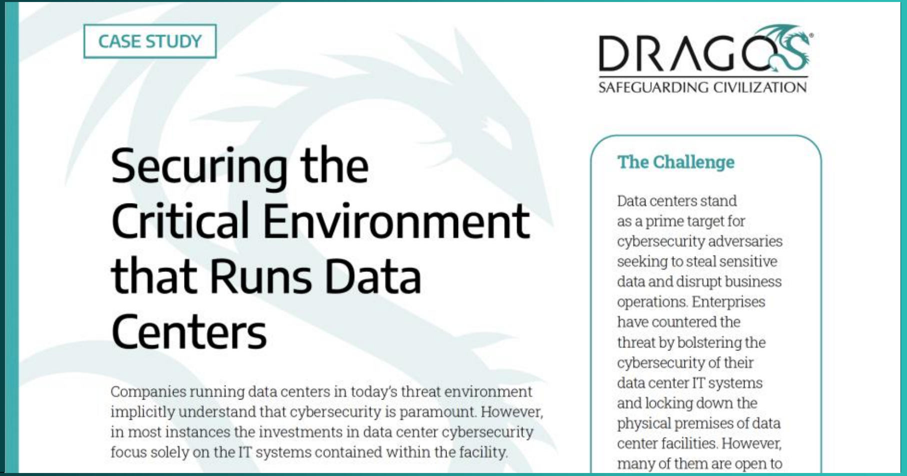
SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

Cybersecurity for Building Automation Systems

Integrated technology, intelligence, and services from Dragos

CASE STUDY



CASE STUDY

DRAGOS
SAFEGUARDING CIVILIZATION

Securing the Critical Environment that Runs Data Centers

Companies running data centers in today's threat environment implicitly understand that cybersecurity is paramount. However, in most instances the investments in data center cybersecurity focus solely on the IT systems contained within the facility.

The Challenge

Data centers stand as a prime target for cybersecurity adversaries seeking to steal sensitive data and disrupt business operations. Enterprises have countered the threat by bolstering the cybersecurity of their data center IT systems and locking down the physical premises of data center facilities. However, many of them are open to

Q&A

QUESTIONS AND ANSWERS